RANDY E. KLEINMAN (CA SBN 320061)
GERSTMAN SCHWARTZ LLP
1399 Franklin Avenue, Suite 200
Garden City, New York 11530
Telephone: (516)880-8170
Facsimile: (516) 880-8171
Email: rkleinman@gerstmanschwartz.com

Attorneys for Plaintiff
ALI AL-AHMED

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

| | |
|---|---|
| ALI AL-AHMED,<br><br>Plaintiff,<br><br>v.<br><br>TWITTER, INC.; ALI HAMAD A ALZABARAH<br><br>Defendant | CASE NO.: 3:21-cv-08017-EMC<br><br>**PLAINTIFF'S MEMORANDUM IN OPPOSITION TO DEFENDANT TWITTER, INC.'S MOTION TO DISMISS**<br><br>Date: March 3, 2022<br>Time: 1:30 p.m.<br>Dept: Courtroom 5, 17th Fl<br>Judge. Hon Edward M. Chen<br><br>Date Filed: October 13, 2021<br>Trial: None Set |

## TABLE OF CONTENTS

**Page**

**Table of Authorities**

**Cases**

**Statutes**

## BACKGROUND AND FACTS

Plaintiff respectfully refers the Court to his Complaint, which has a detailed recitation of the facts [*see* ECF Doc. 1], along with Plaintiff's supporting Declaration. *See* Ex. A.

## ARGUMENT

"[U]nder the federal rules a complaint is required only to give the notice of the claim such that the opposing party may defend himself or herself effectively." *Starr v. Baca*, 652 F.3d 1202, 1212 (9th Cir. 2011). Detailed factual allegations are not required; rather, a complaint must only allege sufficient facts to "state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 547 (2007). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Twombly*, 550 U.S. at 556). When reviewing a motion to dismiss under Fed. R. Civ. P. 12(b)(6), courts "accept[] factual allegations in the complaint as true and construe[] the pleadings in the light most favorable to the nonmoving party." *Colony Cove Props., LLC v. City of Carson*, 640 F.3d 948, 955 (9th Cir. 2011).

### I. Plaintiff Has Article III vis-à-vis Twitter's Invasion of Plaintiff's Statutory Right to Privacy.

#### a. Plaintiff Has Established A Causal Connection.

Where, as here, one private party accuses another of invading a personal legal right conferred on him by statute and causes substantial pecuniary harm, a case or controversy exists. Plaintiff alleges, *inter alia*, that by intercepting, reviewing, collecting, storing and disseminating Plaintiff's private messages and data, Defendant Twitter, Inc. ("Defendant" or "Twitter") invaded his legal rights under California Constitution Article I, Section I, and in violation of various and sundry state shield laws including, *inter alia,* California's Shield Law in Article I, Section 2(b) of the California constitution, and Washington, D.C.'s Free Flow of Information Act under D.C. Code

§§ 16-4701, et seq. Plaintiff alleges that Defendant was complicit or otherwise reckless in allowing this to occur and that Defendant continues to invade his privacy. This establishes a causal connection between Defendant's conduct and Plaintiff's harm and gives him Article III standing to sue over that personal violation without needing to show consequential harm and notwithstanding the substantial financial harm he sustained. *See Spokeo v. Robins*, 136 S. Ct. 1540 (U.S. 2016).

**b. Plaintiff Has Alleged A Concrete And Particularized Invasion Of His Statutory Rights By Twitter.**

Statutory rights are as worthy of judicial protection as common-law and constitutional rights because "there is absolutely no basis for making the Article III inquiry turn on the source of the asserted right." *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 576 (1992). Accordingly, "the actual or threatened injury required by Art [icle] III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing." *Havens Realty Corp. v. Coleman,* 455 U.S. 363, 373 (U.S. 1982) (internal quotations omitted). For that reason, "[standing's] existence in a given case is largely within the control of Congress." Scalia, *supra,* at 885.

In *Spokeo v. Robins*, 136 S. Ct. 1540 (U.S. 2016), the Supreme Court held that for an injury to be "particularized" it "must affect the plaintiff in a personal and individual way" and that Plaintiff's personal interest in the handling of his credit information pursuant to the Fair Credit Reporting Act ("FCRA") satisfied that requirement. *Id.* at 1548. The Court further held that "a plaintiff may establish standing through allegations of violation of a statutory right" (*Gaos v. Google, Inc.*, 2011 WL 7296480, *3 (N.D. Cal., Apr. 7, 2011)) so long as the plaintiff demonstrates a "concrete interest" connected to the statutory right. *Spokeo*, 136 S. Ct. at 1549. Upon remand, the Ninth Circuit determined that because the FCRA was crafted to protect consumers like the plaintiff, and the defendant's violation of the statute could be harmful to the plaintiff, his alleged

injuries were sufficiently concrete to satisfy the injury-in-fact requirement. *Robins v. Spokeo, Inc.*, 867 F.3d 1108, 1113 (9th Cir. 2017).

Here, application of these principles shows that Plaintiff has Article III standing and, because we are at the pleading stage, his allegations must be treated as true. *Warth v. Seldin*, 422 U.S. 490, 521 (1975). First, as articulated in Plaintiff's affidavit, "as a freelance journalist and author this has cost me hundreds of thousands of dollars in lost revenue from writing articles and books and through podcasts." Exhibit A at ¶14. Second, the California Constitution provides a private right of action against non-government actors for violations of the right of privacy: "All people are by nature free and independent and have inalienable rights. Among these are ... pursuing and obtaining ... privacy." Cal. Const., Art. I Section 1. That is the claim Plaintiff brought. In particular, he alleges that by intercepting, reviewing, collecting, storing and disseminating his private messages and data, Defendant invaded his legal rights under California Constitution, among other things, and that Defendant was willfully complicit in these acts and continues to act in bad faith. Complaint at ¶¶ 15; 19-23; 26; Fn. 7; *see also* Exhibit A. The Complaint thereby alleges that Plaintiff's concrete statutory right was "affect [ed] in a personal and individual way." *Lujan,* 504 U.S. at 560 n.1; *see id.* at 581 (Kennedy, J., concurring in part and concurring in the judgment) (same); *see also Spokeo*, 136 S. Ct. at 1549. Because Plaintiff alleges that *his* statutory rights were invaded when *his* privacy was invaded, Plaintiff's claim that Defendant violated the California Constitution "will be resolved, not in the rarified atmosphere of a debating society, but in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action." *Lujan,* 504 U.S. at 560 (citations omitted).

After detailing many ways in which Defendant violated Plaintiff's right to privacy and committed other various tortious acts, the Complaint alleges that Defendant willfully and continually failed to follow/implement reasonable procedures that are designed to assure that it

protects its users. Complaint at ¶¶ 15-27; 47-49. Plaintiff met his burden to plead Article III standing. *See Spokeo*, 136 S. Ct. at 1549; *Lujan,* 504 U.S. at 561 ("At the pleading stage, general factual allegations of injury resulting from the defendant's conduct may suffice, for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim.") (citations omitted).

In addition, Defendant cannot reasonably contest that the injury alleged by Plaintiff "is fairly traceable to the challenged action of the defendant" and "will be redressed by a favorable decision." *Friends of Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.,* 528 U.S. 167, 180-81 (2000). As to traceability, the Complaint alleges that Defendant's willful failure to follow its Terms of Service ("TOS"), violations of California statutes and its constitution, as well as complicity in the acts undertaken against him resulted in the unlawful invasion of privacy. Complaint at ¶¶ 15-27. That is sufficient: Plaintiff need not "establish"—let alone plead—"with any certainty" that Plaintiff's account would not have been breached and/or terminated if Defendant had followed the proper procedures. *Spokeo*, 136 S. Ct. at 1549; *Lujan,* 504 U.S. at 572 n.7; *Massachusetts v. E.P.A.,* 549 U.S. 497, 518 (U.S. 2007) ("A [litigant] who alleges a deprivation of a procedural protection to which he is entitled never has to prove that if he had received the procedure the substantive result would have been altered. All that is necessary is to show that the procedural step was connected to the substantive result.") (citations omitted).

## II. Plaintiff's Claims Are Not Time-Barred

### a. Plaintiff Did Not and Could Not Have Known About the KSA's Hack Until it Was Disclosed in the November 2019 Indictments.

Pursuant to the "discovery rule," a claim accrues when a "plaintiff discovers, or has reason to discover, the cause of action." *Garamendi v. SDI Vendome S.A.*, 276 F. Supp. 2d 1030, 1038 (C.D. Cal. 2003). "[A] plaintiff is held to discover her cause of action when she suspects or should

suspect that her injury was caused by wrongdoing." *Id.* Citing to *Fox v. Ethicon Endo-Surgery, Inc.*, 35 Cal.4th 797, 807 (2005), Twitter argues that "[t]he discovery rule does not delay accrual in that situation because the identity of the defendant is not an element of a cause of action." But Twitter fails to mention that the *Fox* court "distinguished between ignorance of the identity of the defendant and ignorance of the cause of action based on the commonsense assumption that once the plaintiff is aware of the latter, he normally has sufficient opportunity, within the applicable limitations period, to discover the identity of the former." *Id.* (citations omitted). Thus, the discovery rules "delays accrual until the plaintiff has, or should have, inquiry notice of the cause of action." *Id*. "Traditionally at common law, a "cause of action accrues when [it] is complete with all of its elements—those elements being wrongdoing, harm, and causation." *Aryeh v Canon Bus. Solutions, Inc.*, 55 Cal 4th 1185, 1191 (2013) (citations omitted). Moreover, "[t]he doctrine of fraudulent concealment tolls the statute of limitations where a defendant, through deceptive conduct, has caused a claim to grow stale. *Regents of University of California v. Superior Court*, 20 Cal.4th 509, 533 (1999).

Here, as Plaintiff's Affidavit makes clear, he never received any notice from Twitter in December 2015 despite carefully checking all of his emails, including his spam folders Ex. A at ¶ ¶ 4-5. Plaintiff likewise attests that he never received an in-app notification, but cannot confirm this because his account was suspended by Twitter. *Id*. Thus, because Plaintiff had no knowledge that his account was hacked, he could not have known that any causes of action exist. Even assuming, *arguendo*, that Plaintiff received the notice, he had no reason to think that KSA had infiltrated Twitter operatives and, along with Twitter's assistance, committed an inside job. Given wide suspicions that Russia, China, and North Korea, among others, have engaged in hacking in the United States, the KSA is hardly the first regime to come to mind in a vaguely worded mention of "government sponsored" cyber-attacks, let alone a regime that Twitter might be in league with.

Thus, even if Plaintiff knew of these so-called "state-sponsored" attacks, he could not have known that such attacks were, at the very least, facilitated by Twitter employees; a fact that Twitter deliberately, and fraudulently, concealed to avoid liability. Twitter's fraudulent concealment of this information therefore tolled the statute of limitations. *Regents*, 20 Cal.4th 509 at 533.

In any event, Twitter's argument that Plaintiff could have discovered Twitter's involvement while Twitter went through great lengths to conceal this information, or that his claims could have accrued before this point, is risible. Insofar as Plaintiff could not establish causation, his causes of action for ECPA, CFAA, SCA, promissory estoppel, intrusion upon seclusion, negligent hiring, and negligence could not have accrued until he learned of Twitter's involvement by virtue of the perpetrators' indictment in November 2019.[1] For example, Plaintiff would have no way of identifying a negligent hiring, retention, and supervision claim if he did not know that Twitter employees were behind the hack.

**b. The Continuous Accrual Doctrine Is An Equitable Exception To The Usual Rules Governing Limitations Periods.**

The continuous accrual doctrine, as applied in *Aryeh v Canon Bus. Solutions, Inc.*, 55 Cal. App. 4th 1185, 1191 (2013), mandates application to every cause of action in this case. Specifically, Plaintiff's claims are timely insofar as they relate to Twitter's conduct during the four years preceding the filing of the Complaint for breach of contract and breach of implied covenant of good faith and fair dealing, three years for fraudulent inducement, and two years for SCA, invasion of privacy, and negligent hiring, and reckless endangerment.

Generally, a "cause of action accrues when [it] us complete with all of its elements—those elements being wrongdoing, harm, and causation." *Id*. at 1191 (2013) (citations omitted). Under

[1] https://www.justice.gov/usao-ndca/press-release/file/1215976/download, *United States v. Ahmed Almutairi*, a/k/a Ahmed Aljbreen; and Ali Alzabarah, November 2019.

the continuous accrual doctrine, however, "a series of wrongs or injuries may be viewed as each triggering its own limitations period, such that a suit for relief may be partially time-barred as to older events but timely as to those within the applicable limitations period." *Id.* at 1192. The California Supreme Court explained that the theory of continuous accrual,

> … is a response to the inequities that would arise if the expiration of the limitations period following a first breach of duty or instance of misconduct were treated as sufficient to bar suit for any subsequent breach or misconduct; parties engaged in long-standing misfeasance would thereby obtain immunity in perpetuity from suit even for recent and ongoing misfeasance. In addition, where misfeasance is ongoing, a defendant's claim to repose, the principal justification underlying the limitations defense, is vitiated. *Id.* at 1198; *see also Gilkyson v Disney Enters., Inc.*, 244 Cal. App. 4th 1336 (2016) (applying continuous accrual doctrine to breach of contract claim).

Here, Defendant refuses to honor—and in fact exploits and breaches—the contractual obligations contained in its TOS (express and implied) including its obligation to preserve Plaintiff's confidential/privileged sources and list of followers, and its obligation to not unreasonably terminate/suspend his Arabic-language Twitter account in which he has a reasonable expectation of privacy. Twitter further breaches its TOS by continuing to keep Plaintiff's Arabic-language Twitter account terminated/suspended without justification, committing fraudulent acts against Plaintiff, and continuing to unlawfully suppress Plaintiff's constitutional rights to Freedom of Speech and Freedom of Assembly. Twitter claims immunity in perpetuity from suit, even for the acts it committed within the past two years and therefore within the relevant statute of limitations period for all causes of action. So, while Twitter continues to engage in various and sundry misfeasance and malfeasance, Plaintiff will be forever barred from recovery. Fortunately, the common law has long "settled that separate, recurring invasions of the same right can each trigger their own statute of limitations." *Aryeh* at 1198.

According to the California Supreme Court, "[t]o determine whether the continuous accrual doctrine applies here, we look not to the claim's label … but to the nature of the obligations allegedly breached." *Aryeh* at 1200. Just as each excess charge triggered its own limitations period in *Aryeh,* each of Twitter's bad acts from December 2015 to the present date have caused ongoing harm to Plaintiff sufficient to satisfy each of the relevant statute of limitations periods. Twitter's ongoing malfeasance targeting Plaintiff includes, but is not limited to, 1) unlawfully accessing his confidential/privileged sources, list of followers, and other proprietary electronic data/intellectual property ("IP"), and improperly publishing/disseminating same, thereby violating i) the SCA; ii) Plaintiff's right of privacy under the California constitution Article I, Section I; iii) the UCL; iv) the CFAA; and iv) the EPCA; 2) terminating/suspending his Arabic-language Twitter account and withholding his confidential/privileged sources and list of followers, in violation of the UCL; 3) breaching contractual obligations (express and implied) contained in Twitter's TOS including the implied covenant of good faith and fair dealing; 4) deliberately/negligently/recklessly employing operatives who continue to commit tortious acts against Plaintiff; 5) engaging in fraud including, but not limited to, making materially false statements regarding its obligations to and relationship with Plaintiff; and 6) violating Plaintiff's First Amendment right to Free Speech and Freedom of Assembly.

**c. Each Of Twitter's Deliberate/Negligent/Reckless Acts Constitute A Recurring Harm For Which Plaintiff Is Entitled Relief.**

The California Supreme Court "long settled that separate, recurring invasions of the same right can each trigger their own statute of limitations." *Aryeh* at 1198. "When an obligation or liability arises on a recurring basis, a cause of action accrues each time a wrongful act occurs, triggering a new limitations period." *Hogar Dulce Hogar v. Community Development Commission* 110 Cal.App.4th 1288, 1295 (2003). Because each deliberate/negligent/reckless act provides all

the elements of Plaintiff's claims—wrongdoing, harm, and causation (*Pooshs v. Philip Morris USA, Inc.*, 51 Cal. 4th 788 (2011))—each may be treated as an independently actionable wrong with its own time limit for recovery. *Aryeh*, at 1198-1199.

**III. CDA Section 230(c)(1) Does Not Bar Plaintiff's Account Suspension-Related Claims.**

Recently, in October 2020, Justice Thomas published a concurrence in a decision denying certiorari, excoriating courts for applying CDA Section 230 too broadly. *See Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC*, 2020 U.S. LEXIS 4834 (U.S. 2020). Justice Thomas notes that "by construing §230(c)(1) to protect *any* decision to edit or remove content, courts have curtailed the limits Congress placed on decisions to remove content. *Id*. at *10 (internal citations omitted) (emphasis in original); *see also e-ventures Worldwide, LLC* v. *Google, Inc.*, 2017 U.S. Dist. LEXIS 88650 (M.D. Fla. 2017) (rejecting the interpretation that §230(c)(1) protects removal decisions because it would "swallo[w] the more specific immunity in (c)(2)"). As Justice Thomas poignantly laments, "[w]ith no limits on an Internet company's discretion to take down material, §230 now apparently protects companies who racially discriminate in removing content." *Malwarebytes, Inc.*, at 10.

Notably, Justice Thomas expresses skepticism about Section 230's use to protect companies from a wide array of traditional product defect/design flaw claims; that is, claims arising from a defendant's own misconduct. *Id.* at 10-12; *see also Biden v Knight First Amendment Inst. at Columbia Univ.*, 141 S. Ct. 1220, 1227, fn.5 ("Threats directed at digital platforms can be especially problematic in the light of 47 U. S. C. §230, which some courts have misconstrued to give digital platforms immunity for bad-faith removal of third-party content."). In fact, examples of courts extending Section 230 immunity overbroadly abound. *Id.* at 12. "A common thread through all these cases is that the plaintiffs were not necessarily trying to hold the defendants liable 'as the publisher or speaker' of third-party content. §230(c)(1). Nor did their

claims seek to hold defendants liable for removing content in good faith. §230(c)(2)." *Id*. Rather, as here, these claims emanated from the defendants' own misconduct. Particularly relevant to the instant matter:

> *[p]aring back the sweeping immunity courts have read into §230 would not necessarily render defendants liable for online misconduct. It simply would give plaintiffs a chance to raise their claims in the first place*. Plaintiffs still must prove the merits of their cases, and some claims will undoubtedly fail. Moreover, States and the Federal Government are free to update their liability laws to make them more appropriate for an Internet-driven society.
>
> *Extending §230 immunity beyond the natural reading of the text can have serious consequences*. Before giving companies immunity from civil claims for "knowingly host[ing] illegal child pornography," *Bates*, 2006 U.S. Dist. LEXIS 93348, 2006 WL 3813758, *3, or for race discrimination, *Sikhs for Justice*, 697 Fed. Appx., at 526, we should be certain that is what the law demands.
>
> Without the benefit of briefing on the merits, we need not decide today the correct interpretation of §230. But in an appropriate case, it behooves us to do so. *Malwarebytes, Inc.*, at 12-13 (emphasis added).

**a.Twitter's Conduct Is Anathema To CDA Section 230(c) And Its Stated Policies And Therefore Does Not Fall Within Its Ambit.**

Defendant alleges that Plaintiff's claims arising from Defendant's suspension of his Arabic-language Twitter account for violation of the SCA, breach of contract, civil conspiracy, and replevin, are immune from liability under Section 230(C)(1). But Defendant's behavior, and its interpretation of Section 230(c), which would provide immunity to any user or provider of interactive computer services blocking any content for any reason, flies in the face of each of Section 230's stated policies including, 1) the promotion of the "continued development of...interactive computer services"; 2) the preservation of "the vibrant and competitive free market"; 3) the encouragement of "the development of technologies which maximize user control"; 4) the protection of children from obscene content online; and 5) the enforcement of Federal criminal laws. 47 U.S.C. § 230(b).

Defendant's construction of Section 230 and its extension of the statutory immunity provided under Section 230(c) to Defendant's actions run afoul of each of these policies and the fundamental purposes of the CDA. *See Collins v. Gee W. Seattle LLC*, 631 F.3d 1001, 1005 (9th Cir. 2011) ("[W]e may not read a statute's plain language to 'produce a result contrary to the statute's purpose or lead to unreasonable results.'" (quoting *U.S. v. Combs*, 379 F.3d 564, 569 (9th Cir. 2004)); *cf. Hernandez v. Williams, Zinman & Parham PC*, 829 F.3d 1068, 1073 (9th Cir. 2016) ("The words of a statute are, of course, dead weights unless animated by the purpose of the statute.").

The Ninth Circuit has been particularly dubious of large Internet companies seeking special privileges under the CDA:

> The Internet is no longer a fragile new means of communication that could easily be smothered in the cradle by overzealous enforcement of laws and regulations applicable to brick-and-mortar businesses. Rather, it has become a dominant - perhaps the preeminent - means through which commerce is conducted. And its vast reach into the lives of millions is exactly why we must be careful not to exceed the scope of the immunity provided by Congress and thus give online businesses an unfair advantage over their real-world counterparts, which must comply with laws of general applicability.

*Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1164 n.15 (9th Cir. 2008). Given the Congressional policies set forth in Section 230(b), no reason exists to immunize Defendant's behavior solely because it takes place on the Internet rather than on the streets or in peoples' homes. Indeed, "[t]he Communications Decency Act was not meant to create a lawless no-man's-land on the Internet." *Id.* at 1164.

**b. The Court's Extension Of Immunity To Twitter Does Not Advance The Statutory Purpose Of Restricting Access to Indecent Materials.**

Defendant's statutory construction is also at odds with another stated policy of Section 230: the protection of children from exposure to pornographic and obscene material. Section 230(b)(4)

seeks to "remove disincentives" to the development of "blocking and filtering technologies" that would "empower parents to restrict their children's access to objectionable or inappropriate online material"; sub-section (b)(5) seeks to "ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." 47 U.S.C. § 230(b)(4)-(5); *see also Zango, Inc. v. Kaspersky Lab, Inc.*, 568 F.3d 1169, 1173 ("The CDA was enacted to control the exposure of minors to indecent material on the Internet.") (citation omitted)). These statutory policies render illogical the extension of immunity to Defendant and its efforts to impede Plaintiff's access to his Twitter account – which bear no relationship to obscene materials and, to the contrary address, *inter alia*, the injustices faced by Saudi citizens. "Section 230 is captioned 'Protection for 'Good Samaritan' blocking and screening of *offensive* material,' yet another indication that Congress was focused on potentially offensive materials, not simply any materials undesirable to a content provider or user." *Song fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 883 (N.D. Cal. 2015) (emphasis in original). Indeed, it cannot be lost on this Court that what Plaintiff alleges is the antithesis of the conduct of a Good Samaritan protecting children from offensive conduct. What is alleged is complicit self-dealing, or reckless and willful blindness.

In addition, Twitter's purported basis for terminating/suspending Plaintiff's Arabic-language account is a *direct message* Plaintiff allegedly sent to another (currently unknown) user—which Plaintiff unequivocally disavows and also attests is an inaccurate translation[2]—it was a *direct message* – the mere equivalent of a text message and therefore not hosted on Twitter's public platform for public consumption. The principal aim of Section 230 is to protect the children from obscenity and the statute is intended to immunize an interactive service provider for engaging in

[2]*See* Exhibit A at ¶¶6-7 (*e.g.*, "I do not recognize this statement apparently attributed to me by Twitter and which Twitter now alleges was the basis for terminating my Arabic-language account… I would note that certain words used in the direct message attributed to me are colloquial regional expressions that I would never use… In addition, the translation is entirely inaccurate…")

tradition editorial functions in a *public forum*. *See e.g.*, *Force v. Facebook, Inc.*, 934 F.3d 53 (2d Cir. 2019). However, the discrete function of a social medial platform—namely, private messages and the like—could never have been contemplated by the legislature to protect against or require the policing of private exchanges that are very much equivalent to private texts, phone calls or emails. *See Malwarebytes, Inc.*, 2020 U.S. LEXIS at 12-13. Thus, any termination of Plaintiff's account or withholding of his confidential/privileged sources and list of followers should not and cannot be protected by Section 230.

Moreover, a defendant who assists in the development of what made the content unlawful is not protected under Section 230. "For example, a defendant who paid researchers to uncover confidential phone records protected by law, and then provided that information to paying customers, fell within the definition because he did not merely act as a neutral intermediary, but instead 'specifically encourage[d] development of what [was] offensive about the content.'" *FTC v LeadClick Media, LLC*, 838 F.3d 158, 174 (2d Cir 2016) (quoting *FTC v. Accusearch Inc.*, 570 F.3d 1187, 1199 (10th Cir, 2009)); *see also Fair Hous. Council v. Roomates.com*, *LLC*, 521 F.3d 1157, 1167-68 (holding defendant liable for developing content by "not merely…augmenting the content generally, but…materially contributing to its alleged unlawfulness" when it required subscribers to provide information which enabled users of a website to unlawfully discriminate in selecting a roommate). Thus, Defendant's own malfeasance cannot be protected.

Here, Defendant has terminated/suspended the account of a prominent journalist and democracy advocate against one of its most notable shareholders, the KSA. Far from "remov[ing] disincentives" to such developments—the express policy the CDA seeks to foster—Defendant's conduct creates such "disincentives" as it seeks to inhibit and suppress the dissemination of free speech. Allowing, let alone immunizing, such conduct subverts the CDA's policies and purposes. Further, to the extent Twitter is using its ever-changing TOS as a tool to control the participation

of users they do not approve of, such conduct certainly is not protected by the statute. Neither should it be countenanced here. Whether Defendant was willfully complicit, grossly negligent, or just plain negligent remains to be seen. But this certainly presents a question of fact given the strong financial relationship between Defendant and the KSA. This is so despite Twitter's attempts to distance itself from its so-called "rogue employees" and the KSA. *See Biden v Knight First Amendment Inst. at Columbia Univ.*, 141 S. Ct. 1220, 1226 (2001) ("plaintiffs might have colorable claims against a digital platform if it took adverse action against them in response to government threats." This includes threats made by a foreign government).

**c. Defendants Fail To Demonstrate The Requisite "Good Faith" Necessary To Involve Immunity Under CDA Section 230(c)(1).**

The "Good Samaritan" provision under sub-section (A) of Section 230(c)(2) explicitly requires that an "action" "to restrict access" be taken in "good faith." The *entire* CDA Section 230(c), including Section 230(c)(2)(A), is captioned "Protection for '*Good Samaritan*' blocking and screening of offensive material" (emphasis added). It beggars belief that Congress intended to recognize an entity acting in bad faith as a "Good Samaritan," let alone to confer immunity on bad faith conduct. *See Fair Hous. Council of San Fernando Valley v. Roommates.Com, LLC*, 521 F.3d 1157, 1163-64 (9th Cir. 2008) ("[T]he substance of section 230(c) can and should be interpreted consistent with its caption."). Indeed, it would be logically impossible for Congress to have intended to immunize an entity applying "technical means" in bad faith to disable and make unavailable Plaintiff's Twitter account, his list of contacts and effectively his livelihood. So, too, it would be logically impossible for a party to act in good faith if it had in *bad faith* deemed the account/material to be restricted to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." 47 U.S.C. § 230(c)(2)(A). In each case, it would be anomalous in the extreme—and a perversion of the CDA's purposes—if such bad faith conduct

were to be immunized. Thus, contrary to Defendant's argument, it has failed to establish it acted in good faith.

**d. Plaintiff Sufficiently Pleads That Twitter Has Not Acted In "Good Faith."**

This Court should find that Plaintiff has adequately pled that Defendant has *not* acted in "good faith" and cannot therefore claim immunity under Section 230(c)(2). The Complaint alleges, *inter alia* (and it is undisputed), that Twitter employees Ali Hamad Alzabarah ("Alzabarah") and Ahmad Abouammo ("Abouammo") (collectively, "Defendants") were charged by the United States government with being KSA operatives who utilized Twitter resources while on company time to unlawfully access and tamper with Plaintiff's Arabic-language Twitter account, adversely, and substantially affecting his livelihood and jeopardizing the lives of his followers living within the KSA and the surrounding areas. Complaint ¶¶ 21-25; 27-28; 47-49. Plaintiff also alleges that although Defendant tries to play the victim, its conduct was dubious, at best, and constitutes a "ratification or complicity or adoption tailored to appease a neigh beneficial owner to preserve access to a key market – the KSA." Complaint at ¶ 27. Plaintiff further alleges that insofar as Twitter was/is beholden to the KSA, it willfully hired KSA operatives, was complicit in their misconduct, and continues to act in bad faith by, *inter alia*, terminating/suspending Plaintiff's Arabic-language Twitter account and withholding his confidential/privileged sources and list of followers in "its continuing allegiance to the KSA." Complaint at ¶¶ 27-28; 35; Fn. 9. Plaintiff also alleges that this very allegiance to the KSA explains why Defendant upheld Plaintiff's "suspension and kept his account inaccessible" and why they continues to do so to this day: "Twitter is continuing to do the bidding of the KSA; preferring access to the Kingdom and funding from the Kingdom over human rights, freedom and to abiding by the terms of its…agreements

made with Twitter subscribers, and in contravention of its public representation that Twitter is committed to protecting Twitter uses." Complaint at 28.

In short, the Complaint sets forth clear allegations that go far beyond the specificity required under the applicable notice-pleading standards and support a plausible inference that Defendant's suspension and blocking of Plaintiff's account was not undertaken in good faith. Twitter and other social media giants are free to exercise traditional editorial functions, in good faith, filtering content that are in fact akin to "obscene, lewd, lascivious, filthy, excessively violent, [and] harassing" content. They may not, however, target users with demonstrably false allegations and prohibit their users from innocuously exercising their right to Free Speech. Extending immunity in such circumstances regardless of whether Defendant acted on a malicious whim or in bad faith, would effectively allow *anyone* to block *any content* on the Internet *for any reason* as long as the blocking entity was willing to claim the blocked material was "objectionable" pursuant to its own undefined, arbitrary, and entirely personal standards. Defendant's reading of Section 230 conflicts with the Congressional policies stated in the CDA, conflicts with the language and purpose of Section 230, and warrants denial. Allowing global technology giants like Twitter—which effectively operate as public utilities—to operate outside the confines of the law, opens a Pandora's box from which a black hole of horrors will emerge and subsume our basic fundamental liberties.

**e. Twitter's conduct violates the Lanham Act**.

While not expressly alleged as a cause of action in Plaintiff's Complaint, the facts therein sufficiently set forth a Lanham Act claim.[3] Specifically, the Complaint alleges that Twitter

[3] Plaintiff respectfully requests the opportunity to amend his Complaint to formally add, among other things, a Latham Act claim.

"continue[s] to carry the KSA's mission by doing violence to truth and free speech, and by denying Plaintiff access to his proprietary list of followers, research and other intellectual property." Complaint at ¶ 34. Certainly, Plaintiff's interference with prospective economic advantage claim is one "pertaining to intellectual property" within the meaning of Section 230(e)(2) of the CDA's exception to immunity for intellectual property claims. *See* 47 U.S.C. § 230(e)(2).

Even if Section 230(c)(2) immunity was available to Defendant despite its blatant bad faith conduct, which it is not, that immunity would *not* apply to Plaintiff's Lanham Act claim. Section 230(e)(2) provides that "nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2). "[O]n the basis of th[is] statutory text, ... the CDA does not bar [a § 43(a)] Lanham Act claim." *Enigma Software Grp. USA v. Bleeping Computer LLC*, 194 F. Supp. 3d 263, 273-74 (S.D.N.Y. 2016); *see also Gucci Am., Inc. v. Hall & Assocs.*, 135 F. Supp. 2d 409, 413 (S.D.N.Y. 2001) (holding that CDA immunity did not extend to, *inter alia*, claims for "false designations of origin and false descriptions and representations under Section 43(a) of the Lanham Act").

## IV. Twitter's Status As An Information Fiduciary, Imposes a Heightened Standard of Liability.

### a. Twitter is Vicariously Liable For Alzabarah and Abouammo's Conduct.

#### i. As An Information Fiduciary, Twitter Has A Heightened Standard Of Hiring, Retaining, And Supervising Its Employees.

Liability for negligent hiring, retention and supervision requires proof that the employer knew, or should have known, facts which would warn a reasonable person that the employee presents an undue risk of harm to third persons in light of the work to be performed. *Phillips v. TLC Plumbing, Inc.* 172 Cal.App.4th 1133 (2009).

That Twitter—a global technology behemoth with virtually limitless resources—purportedly failed to implement adequate internal controls over its employees, when the very

nature of its business is predicated on being a leader in such technologies, not only strains credulity but furthers Plaintiff's contention that Twitter was complicit in Abouammo's and Alzabarah's conduct. Twitter's assertion that it did not have knowledge that Alzabarah and Abouammo could not be trusted and/or posed a particular risk is entirely speculative and only raises questions of fact. Moreover, Defendant relies on sexual/physical cases to support its argument, which are uniquely predicated on whether an employee knew or should have known about an employee's dangerous propensity due to the existence of a prior criminal record. *See*, *e.g.*, *Juarez v Boy Scouts of Am., Inc.*, 81 Cal. App. 4th 377, 395, (2000). Here, Plaintiff's account was not "hacked" per se, but rather it was quite easily breached by two Twitter employees who were granted unfettered access. Even assuming, *arguendo*, that Defendant was not complicit in these acts, the breach of Plaintiff's account was entirely foreseeable given the unrestricted access afforded to these individuals, the lack of adequate supervision, and the utter dearth of any internal control mechanism to monitor employees' conduct. The fact that Twitter was apparently "unaware" that this was happening only provides further support for this argument and its so-called corrective action was too little too late.

Twitter's is in the business of online global communication. Not only does Twitter have the duty to protect all of its users, it has the technological capacity to do so. As both a matter of law and commons sense, Twitter has a duty to ensure that, 1) its employees are suitable for the job; 2) its employees are adequately supervised/monitored; and 3) appropriate safeguards are in place to ensure that employees do not violate Twitter's TOS, internal rules or any other law. Twitter breached these duties when it hired, retained and failed to adequately supervise Alzabarah and Abouammo, leading to the breach and release of Plaintiff's confidential/privileged sources and list of followers and the termination/suspension of his Arabic-language account.

Accordingly, the portion of Defendant's motion seeking to dismiss Plaintiff's negligent hiring, retention and supervision claim should be dismissed.

**ii. Twitter Ratified Alzabarah and Abouammo's Conduct**

Under California law, "an employer may be liable for an employee's act where the employer either authorized the tortious act or subsequently ratified an originally unauthorized tort." *C.R. v Tenet Healthcare Corp.*, 169 Cal. App. 4th 1094 (2009). Ratification can occur "expressly or it may be adopted by implication based on conduct of the purported principal from which an intention to consent to or adopt the act may be fairly inferred." *Dickinson v Cosby*, 37 Cal. App. 5th 1138, 1158 (2019). Moreover, as described *supra*, Twitter is an information fiduciary and its special power over its users, and its special relationship to its users, creates special duties to ensure that it does not harm the interest of its users. *See Information Fiduciaries* at 1186, *supra*; *see also Knight Securities, LP v Fiduciary Trust Co.*, 5 AD3d 172 (1st Dep't 2004) (a determination of whether a special fiduciary relationship exists is highly fact-specific and typically not resolvable at the pleading stage).

Contrary to Defendant's contentions, the Complaint is replete with allegations that Twitter was/is complicit in and/or ratified the conduct of its KSA operative employees Alzabarah and Abouammo, and continues to be complicit in its employees' unlawful/tortious conduct by keeping Plaintiff's Arabic-language Twitter account terminated/suspended and withholding his confidential/privileged sources and list of followers in "its continuing allegiance to the KSA." Complaint at ¶¶ 21; 24-28; 31, 35, fn. 9 (*see e.g.*, ¶ 24, alleging, in pertinent part, that "Twitter surreptitiously aided and abetted Alzabarah and Abouammo by, among other things, 1) providing them with unfettered access to Twitter's vast resources and infrastructure at the behest of the KSA and with the full knowledge that they would exploit these privileges by improperly gaining access to the accounts of Twitter users, such as Mr. Al-Ahmed, who were adverse to the Saudi regime;

2) helping Alzabarah and Abouammo operate their clandestine operation undetected until they were no longer of use to Twitter and/or the KSA; 3) helping Alzabarah and Abouammo provide the ill-gained information to the KSA; 4) and covering up their malfeasance by purging its internal database of any incriminating evidence and thereafter publicly renouncing Alzabarah and Abouammo's conduct.").

Defendant's claims that the "Complaint concede that Twitter had ***no*** knowledge of Abouammo and Alzabarah's actions" is patently false, as nowhere in the Complaint is any such concession made. That Defendant ostensibly took remedial measures, purportedly cooperated with federal authorities, and supposedly sent Plaintiff notifications of the data breaches does not exculpate Defendant for its misfeasance and malfeasance. Indeed, the facts show just the opposite: that in late 2015, the FBI told Twitter it had a KSA mole (Alzabarah) and that the sensitive investigation was at an early stage. *The FBI explicitly asked Twitter to not tell Alzabarah what was going on as it could hurt the investigation. Yet, Twitter told him anyway*. Justice Department officials were furious with Twitter for ruining their case against Alzabarah, who remains out of American reach.[4] Despite having authority and ability to detain Alzabarah for officials to arrest him after he admitted to crimes, Twitter suspended him, reclaimed the company laptop, and escorted him out. *He fled the US the next day and escaped justice*. In turn, Defendant allowed Abouammo to continue to inappropriately access information inside Twitter until March 1, 2016.

Similarly, Defendant's attempt to minimize its relationship with the KSA is unavailing and does not vitiate the KSA's substantial ownership interest in Twitter at this time.[5] At the very least,

---

[4] Bradley Hope & Justin Scheck, "A Saudi Prince's Attempt to Silence Critics on Twitter". https://www.wired.com/story/mohammed-bin-salman-twitter-investigation/ Last visited January 11, 2021.

[5] Saudi Prince Alwaleed Bin Talal Bin Abdulaziz Alsaud is Twitter's second largest shareholder and owns more shares than its founder and CEO Jack Dorsey. *See This Saudi Prince now owns more of Twitter than Jack Dorsey does*. https://qz.com/519388/this-saudi-prince-now-owns-more-of-twitter-than-jack-dorsey-does/ Indeed, this likely explains Twitter's ongoing campaign to silence and censor critics and political pundits who fail to tow the company line on its forum.

these issues present questions of fact that can only be resolved through further discovery and/or a finder of fact. Defendant's additional contention that it cannot be held liable under a *respondeat superior* theory is also erroneous. Although Defendant argues that Plaintiff fails to allege facts that support Twitter ratified Alzabarah and Abouammo's conduct, certainly its willful obstruction of the FBI's investigation, which led to Alzabarah's escape from justice, evidences Twitter's ratification of these individuals'' conduct. Moreover, while spying itself was ostensibly against Twitter's policies, it is a far cry to allege that Alzabarah and Abouammo's conduct was a detour from their daily responsibilities given that enjoying special access to Twitter's infrastructure, data, and information systems was not just within the scope of their respective job duties, it was their job. Thus, the problem is not simply that Alzabarah and Abouammo accessed and deprived Plaintiff of access to his account and confidential/privileged sources and list of followers, it is that they weaponized this data with impunity. It would be premature to rule that Defendant is not vicariously liable for its employees' conduct before any meaningful discovery has taken place. This is particularly true given that Defendant has unilateral access to information related to its knowledge and/or complicity in its employees' acts. At the very least, Defendant's course of conduct—notwithstanding its assertions of federal cooperation (which are disputed by the facts)—amounts to ratification because it continues to punish Plaintiff by terminating/suspending his account and withholding his confidential/privileged sources and list of followers.

Moreover, Twitter either misses or simply ignores the point that the most fundamental aspect of its security apparatus is to restrict access to users' private information to those very few employees who actually need it. Twitter's failure to do this means that it negligently supervised nearly everyone who had unneeded access, including Abouammo and Alzabarah. Plaintiff need

only show it was reasonably foreseeable that someone in a company with 3,900 employees might do this, similar to what has already occurred at Google. Second, industry-standard security required a system that generated real-time warning alerts when invasions of private user data occurred. A system without such warning alerts—which people would necessarily have to heed to—unequivocally falls short of industry standards and constitutes failure to supervise. Twitter's disregard of the warning alerts that their security system was generating constituted at least negligent supervision/retention of the two employees that were invading private user data for KSA.

Beginning in December 2014 for Abouammo and May 2015 for Alzabarah, their improper accessing of private user data was setting off alerts in Twitter's security system. If Twitter was paying attention to those alerts instead of ignoring them or looking the other way, it would have investigated the two, which would have revealed that they were improperly accessing private user data for KSA. This would have been even more apparent for Alzabarah, who invaded some 6,000 sets of private account information, ostensibly for work purposes, while he stayed in Saudi Arabia during a month-long personal leave from Twitter. Twitter utterly failed to supervise the two KSA spies in its employ by failing to monitor the alerts and as a result, negligently retained them without curtailing their improper access to private user data. KSA, a large investor in Twitter, must have been thrilled.

Accordingly, the portion of Defendant's motion seeking to dismiss Plaintiff's ECPA, CFAA, SCA, UCL, unjust enrichment, breach of contract, promissory estoppel, and intrusion on seclusion claims in their entirety should be denied.

**b. Twitter Cannot Hide Behind Its Vague And Ambiguous Service Terms.**

The crux of Defendant's argument is that its TOS treats personal privacy as an entitlement that end-users have consented to surrender and have no right to control. This argument, however, has been largely rejected because social media users generally do not understand the cumulative

effects of such agreements, which ultimately leave their privacy largely under-protected.[6] These users also cannot rely on traditional contract law alone to adequately protect their information privacy interests, at least with regard to websites with privacy policies.[7] Because Twitter users understand that their personal data may be collected and that Twitter's methods are beyond their understanding, they seek reassurance that using its services are safe. But the details of Twitter's—ever-changing—privacy policies are buried within the fine print of its TOS and in the code of the company's information infrastructure.[8] Although the details of Twitter's privacy policies are technically public, the meaning and practical consequences are not easy for the average user, such as Plaintiff, to understand. Yet another type of information asymmetry lies in the fact that Twitter's information infrastructure is kept secret. By presenting itself as a trustworthy custodian of users' private data, and by emphasizing that in order to maintain security and competitiveness it cannot be fully transparent, Twitter induces relations of trust from its users so that its users will continue to use its services. As a result, new types of fiduciary relationships and fiduciary obligations arise that are recognizable under the law and which require companies like Twitter to protect more things than they expressly set out in their TOS. This is particularly true given that Twitter's TOS/privacy policies are vague and ambiguous

---

[6] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L.J. 1131, 1149 (2011) ("Many consumers have little idea how much of their information they are giving up or how it will be used."); A. Michael Froomkin, *The Death of Privacy?*, 52 Stan. L Rev. 1461, 1502 (2000) ("[C]onsumers suffer from privacy myopia: they will sell their data too often and too cheaply."); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 Stan. L Rev. 1393, 1452 (2001) ("It is difficult for the individual to adequately value specific pieces of personal information."). Information and learning costs often deter effective contracting. *See, e.g.*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in Consumer Protection In The Age Of The "Information Economy"*, 341, 360-61 (Jane K. Winn ed., 2006) (noting that privacy policies are often difficult to understand and therefore most Americans do not read them).

[7] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 596 (2014).

[8] *See, e.g.*, Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year would Take 76 Work Days, ATLANTIC* (Mar. 1, 2012), http://www.theatlantic.com/ technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would- take-76-work-days/253851/ ("The collective weight of the web's data collection practices is so great that no one can maintain a responsible relationship with his or her own data.").

and fail to adequately warn its users how their data can be used. *See* Cal. Civ. Code § 1654 ("the language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist.").

Twitter must be held accountable for violating its own privacy policies and cannot be permitted to continue its con game – gaining the trust and confidence of its users in order to act against the users' interests later on.[9] Indeed, the premise of a con game is just the mirror image of the concept of a fiduciary duty: if Twitter induces a user to treat it with confidence, Twitter cannot turn around and betray that confidence.[10] At a minimum, because Twitter holds itself out as trustworthy and encourages the disclosure of personal information that places its users in a vulnerable position, it should be held accountable for its representations. Twitter, as an information fiduciary, must be held to a reasonable ethical standard of trust and confidentiality, irrespective of whether it makes specific representations.

To this end, Twitter's termination/suspension of Plaintiff's Arabic-language account was entirely unjustified. Twitter's alleged basis for terminating Plaintiff's account is a direct message allegedly sent to another user whom Twitter has not revealed the identity of nor revealed the context in which the alleged statement was made. Moreover, Plaintiff disavows any knowledge of this alleged statement and rejects the translation proffered by Twitter in

---

[9] *See* M. Allen Henderson, *Flim-Flam Man: How Con Games Work*, 3 (1985) ("As the term implies, the confidence artist gains the *confidence* of his victim in order to defraud him."); Lionel S. Lewis, *Con GameL Bernard Madoff and His Victims*, 2-3 (2012) ("What all con games have in common is that they attempt to victimize . . . by gaining the confidence of marks or victims.").

[10] *See*, *Information Fiduciaries*, *supra* at 1224, "Online service providers act like con men when they assure people that they will treat them fairly in order to obtain their business — and their data — and then betray them. In confidence games, betrayal may occur in wholly unexpected ways; indeed, if the mark saw the betrayal coming, they would not fall for it. We might make a similar point about the potential dangers of the digital world. Digital businesses are supposed to be creative; that is how they succeed. Yet, one side effect of being creative means that businesses will probably come up with ever new ways to use personal data, and therefore ever new ways to betray their end-users. The point of treating them as information fiduciaries is to encourage creativity without facilitating betrayal."

support of its RJN.[11] That Twitter seems to believe the fine print of its TOS exculpate it from any liability is all well and good; however, as explained above, this does not obviate liability.[12] Plaintiff most certainly had/has a reasonable expectation that his information/account would be protected based upon general market services and, broadly speaking, the reasonable understanding that while using its platform, Twitter would function as Section 230 anticipates rather than the arm of a hostile government or with negligence amounting to same. If a landlord is so laxed that it leaves the front and back door open (as Twitter has done), at some point the landlord is responsible for crimes that occur therein. In like fashion, Twitter has put out a doormat for Saudi operatives to compromise Plaintiff's data and confidential/privileged sources and followers. Twitter has misrepresented itself and its platform, thereby exposing Plaintiff not just to scorn or ridicule but to danger.

## V. Plaintiff's Remaining Causes of Action Are Viable.

### a. Plaintiff States a Claim Under The Wiretap Act

The Wiretap Act provides a private right of action against any person who "intentionally intercepts . . . any wire, oral, or electronic communication." *In re iPhone App. Litig.*, 844 F. Supp. 2d. 1040, 106 (N.D. Cal. 2012) (hereinafter "*iPhone II*")1. The objective of the Wiretap Act is to protect the privacy of communications. *See Gelbard v. United States*, 408 U.S. 41, 48 (1972).

*First*, the Complaint alleges that Twitter intentionally intercepted Plaintiff's "**Tweets, private messages, direct message, online chats, friend requests, file transfers, file uploads, and file downloads**." Complaint at ¶ 54. This is very different than the e-mails Defendant erroneously alleges are at the center of Plaintiff's claims. *See In re Google Inc. Street View Electronic Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1078-79, 1082 (N.D. Cal. 2001) (upholding

[11] *See* Exhibit A at ¶¶6-7 (*e.g.*, "I do not recognize this statement apparently attributed to me by Twitter and which Twitter now alleges was the basis for terminating my Arabic-language account… I would note that certain words used in the direct message attributed to me are colloquial regional expressions that I would never use… In addition, the translation is entirely inaccurate…")

[12] *See, e.g.*, M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1149 (2011) ("Many consumers have little idea how much of their information they are giving up or how it will be used.").

plaintiffs' Wiretap Act claims against Google, stating that "Congress amended the Wiretap Act to provide statutory privacy protection and a civil right of action for interceptions of electronic communications, including, inter alia, computer-to-computer transmissions and electronic mail" and finding that Google "intercept[ed] Plaintiffs' data packets, arguably electronic communications, from Plaintiffs' personal Wi-Fi networks").

*Second*, Defendant's argument that the "nonpublic account information" accessed by its employees does not qualify as "contents" of a communication within the meaning of the Wiretap Act is patently false. Once again, Plaintiff alleges that among other things, his "private messages, direct message, online chats…file transfers, file uploads, and file downloads" were "intercepted." Complaint at ¶ 54. These items very clearly qualify as "contents" of a communication under the Wiretap Act, and Plaintiff's allegations are not merely limited to "email addresses, contacts, phone numbers, birth dates, and [IP] addresses" as Defendant disingenuously claims. *See* 18 U.S.C. § 2510(8) (defining "contents" as "includ[ing] any information concerning the substance, purport, or meaning of that communication"); *In re United States*, 885 F. Supp. 197, 199 (CD Cal 1995).

*Third*, Plaintiff alleges that *Twitter authorized* and was directly responsible for the "intentional" Wiretap Act violations, and is not merely seeking to impute vicarious liability. Thus, Plaintiff has sufficiently alleged a viable Wiretap Act claim.

**b. Plaintiff states a claim under the SCA.**

In 1986, Congress passed the SCA because "the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010) (citing *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008), *rev'd on other grounds sub nom*. *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010)). However, the SCA was enacted "before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994." *Crispin*, 717 F. Supp. 2d at 972 n.15. In addition, by 2008, "nearly 70 percent of people use[d] web-based email, store[d]

data or photos online, or use[d] web-based software programs." *Id*. Because technology has exponentially advanced since the SCA was passed, "[t]he resulting task of adapting the Act's language to modern technology has fallen largely upon the courts." *Id*.

"Under the SCA, an entity providing an electronic communication service to the public 'shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.'" *In re Facebook Privacy Litig.*, No. 10-cv-02389, 2011 WL 6176208, at *2 (N.D. Cal. Nov. 22, 2011) (quoting 18 U.S.C. § 2702(a)(1)). Similarly, 18 U.S.C. § 2701(a) provides, in relevant part, that any person who intentionally exceeds its authorization to access to an electronic communication service is in violation of the SCA. "The [SCA] reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility." *Theofel v. Farey Jones*, 341 F.3d 978, 982 (9th Cir. 2003). "Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents,…the [SCA] protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." *Id.* The SCA prohibits two types of entities from sharing electronically stored information: (1) remote computing services ("RCS"), and (2) electronic communication services ("ECS"). *See* 18 U.S.C.A. § 2702; *Quon*, 529 F.3d at 900-02. Twitter does not dispute that it is an RCS and/or an ECS for purposes of this case. Thus, the SCA applies to Twitter.

Plaintiff has adequately alleged a violation of the SCA. The Complaint alleges that Twitter—without Plaintiff's consent—unlawfully accessed his private messages, direct message, online chats, file transfers, file uploads, and file downloads, thus exceeding the scope of its access pursuant to § 2701(a), and shared Plaintiffs' stored communications with third parties in violation of § 2702(a). Complaint at ¶ 54; 76-78. Twitter argues that its conduct was lawful pursuant to §

2701(c)(1), which provides an exception from the SCA for conduct "authorized...by the [ECS,]" or when authorized by the user of the ECS. This argument is nonsensical. Twitter is the ECS and it cannot authorize itself to access Plaintiffs' communications beyond the authorization it received from Plaintiffs. Twitter's argument that it had authorization—which directly contradicts the Complaint's allegations that Twitter did not have authorization (*e.g.*, ¶ 78)—is circular and is improper on a motion to dismiss. *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008) (plaintiffs' allegations accepted as true on motion to dismiss).

**c. Plaintiff States a Claim Under the CFAA**

The Computer Fraud and Abuse Act ("CFAA") prohibits the transmission of information from and/or the unauthorized access of a "protected computer" resulting in damage or loss (18 U.S.C. §18 U.S.C. § 1030(a)(5)). In addition to federal law, California law also expressly prohibits knowingly and without permission accessing, causing, and/or assisting in the accessing of a computer data and computer system. *See* California Penal Code ("Cal. Penal Code") § 502. "In contrast to the CFAA, the California statute does not require *unauthorized* access. It merely requires *knowing access*." *United States v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016), cert. denied, 137 S. Ct. 628 (2017) (emphasis in original) ("the term 'access' as defined in the California statute includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly."). An individual or entity can be guilty of violating Cal. Penal Code § 502(c) by "assisting in providing means of accessing" and/or "caus[ing] to be accessed any computer, computer system, or computer network." *Id.*

Here, the Complaint alleges that Twitter authorized and assisted the unauthorized access, collecting, and transmitting of Plaintiff's computer and computer data in violation of the CFAA.

**d. Plaintiff States a Claim under the UCL**

Under the UCL, "a practice is prohibited as 'unfair' or 'deceptive' even if not 'unlawful' and vice versa.'" *Cel-Tech Communications, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal. 4th 163, 180 (1999). To recover for Twitter's "unfair" business act or practice, Plaintiff must establish he (1) suffered a "substantial" consumer injury (2) that is not "outweighed by any countervailing benefits to consumers or competition" and (3) which he "could not reasonably have avoided." *Camacho v. Auto Club of S. Cal.*, 142 Cal. App. 4th 1394, 1403 (2006). A "substantial" injury is simply "a violation of another's rights for which the law allows an action to recover damages." *Id.* at 1406. As discussed above, Plaintiff sufficiently pled a substantial, compensable injury from, among other things, Twitter unlawfully accessing and disclosing his confidential/privileged sources, list of followers, and other proprietary electronic data/intellectual property and information. On the second requirement, the Eleventh Circuit has explained that "the injury" from the unfair practice "must not be outweighed by any countervailing benefits to consumers or competition *that the practice produces* ...." *Orkin Exterminating Co., Inc. v. FTC*, 849 F.2d 1354, 1364 (11th Cir. 1988) (italics added, citation omitted).

Twitter argues that Plaintiffs' UCL claim fails because he fails to show that the economic injury he sustained was caused by Twitter. This is false insofar as Plaintiff's complaint is replete with facts and allegations demonstrating how his pecuniary injuries were *caused by* Twitter's conduct. *See* Complaint at ¶¶ 47-49. Moreover, in addition, any violation of law "may serve as the predicate" for a claim under the UCL's "unlawful" prong. *Munson v. Del Taco, Inc.*, 46 Cal. 4th 661, 676 (2009); Cal. Bus. & Prof. Code § 17200. Twitter's practices and conduct, as set forth above, have misled Plaintiff and the public in the past and will continue to mislead in the future. Consequently, Twitter's practices constitute an unlawful, fraudulent, and unfair business practice within the meaning of the UCL. *See* Complaint at ¶¶ 31-34; *Sateriale v. R.J. Reynolds Tobacco Co.*, 2012 WL 2870120, at *10 (9th Cir. 2012).

#### e. Plaintiff States a Breach of Contract Claim

To state a claim for breach of contract, Plaintiff was required to plead: (1) the existence of a contract; (2) his performance; (3) Twitter's breach; and (4) resulting damage to Plaintiff.

*Acoustics, Inc. v. Trepte Constr. Co.*, 14 Cal. App. 3d 887, 913 (1971). Twitter does not dispute that a contract exists[13], or that Plaintiff performed (elements 1 and 2) but only argues that it did not breach the relevant contract (element 3).[14] With regard to element (2), the Complaint contains myriad allegations showing that Twitter breached its User Agreement, Privacy Policy, and TOS with Plaintiff. *See* Complaint at§§ 108-118. Moreover, as discussed above in Section XI(b), because of Twitter's status as an information fiduciary, its TOS do not immunize it from a breach of contract claim stemming from a violation of same.

Additionally, it "is inappropriate at the motion to dismiss stage for this Court to interpret the parties' contract and evaluate the viability of Plaintiff's claims based on the terms of the contract." *Gardner v. RSM & A Foreclosure Servs.*, LLC, No. 12-cv-2666, 2013 WL 1129392, at *3 (E.D. Cal. Mar. 18, 2013); *Lizalde v. Adv. Planning Svcs.*, No. 10-cv-834, 2012 WL 2374882, at *15 n.7 (S.D. Cal. June 22, 2012) (declining to "definitively interpret the contracts" on a motion to dismiss); *Davis v. Chase Bank U.S.A.*, N.A., 650 F. Supp. 2d 1073, 1088 (C.D. Cal. 2009).

**f. Plaintiff states a claim for promissory estoppel**

Despite Defendant's disingenuous contention, "*promissory estoppel is distinct from contract* in that the promisee's justifiable and detrimental reliance on the promise is regarded as a substitute for the consideration required as an element of an enforceable contract." *Signal Hill Aviation Co. v. Stroppe*, 96 Cal.App.3d 627, 640 (1979) (emphasis added). Under the doctrine of promissory estoppel, a "promise which the promisor should reasonably expect to induce action or forbearance of a definite and substantial character on the part of the promisee and which does

[13] *See* Twitter's Motion to Dismiss at pp. 38-39 ("the promises at issue are part of an express written contract between Twitter and Al-Ahmed.").

[14] To the extent that Twitter contests damages (element 4), that argument is addressed in Section I (Article III standing) herein.

induce such action or forbearance is binding if injustice can be avoided only by enforcement of the promise." (*C & K Engineering Contractors v. Amber Steel Co.* 23 Cal.3d 1 (1978) (citations omitted). Thus, unlike contract law, which enforces promises because the parties have bargained for and agreed to be bound by them, promissory estoppel is an "alternative theory of recovery" that enforces promises because the promisee has justifiably and foreseeably relied on the promise and equity demands enforcement to avoid injustice. *Division of Labor Law Enforcement v. Transpacific Transportation Co.*, 69 Cal.App.3d 268, 275 (1977). A plaintiff is "entitled to plead theories of recover under separate counts. *Savage v Marle* , 39 Cal App 3d 241, 245, (1974). Because Plaintiff adequately alleges that Twitter made promises in its Privacy Policy and Rules that induced him to rely on these promises "that the identities to and the substances of these communications would be obtained and/or mined by KSA spies to harm and silence KSA critics", he has stated a valid claim for promissory estoppel. Complaint at ¶¶ 120-123.

**g. Plaintiff States A Viable California Invasion of Privacy Act Claim.**

The California Constitution provides a private right of action against non-government actors for violations of the right of privacy: "All people are by nature free and independent and have inalienable rights. Among these are ... pursuing and obtaining ... privacy." Cal. Const., Art. I Section 1. The ballot argument for the initiative that created the right to privacy said that the law "prevents government and business interests from collecting and stockpiling unnecessary information about us and or misusing information gathered for one purpose in order to serve other purposes or to embarrass us." *Hill v. Nat'l Collegiate Athletic Assn.*, 7 Cal. 4th 1, 27 (1994). Defendant's interception, review, theft, scanning, collection, storage, and dissemination of the Plaintiff's confidential/privileged sources and list of followers, without Plaintiff's consent for Defendant's own nefarious purposes is precisely the type of practice the constitutional right to privacy was meant to prohibit.

Plaintiff alleges all three requirements for asserting the claim: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012). Plaintiff alleges that he has a legally protected privacy interest in, 1) the content of direct (non-public) communications of a personal, sensitive and, in certain instances, life or death nature he had with Twitter users inside the KSA and its surrounding areas; 2) the personal (non-public) information/identity of his Twitter contacts within the KSA and its surrounding areas, many of whom were/are Plaintiff's confidential sources protected by, *inter alia*, California's Shield Law in Article I, Section 2(b) of the California constitution, the Free Flow of Information Act, D.C. Code §§ 16-4701, et seq.; 3) Plaintiff's own *non-public* personally identifying information including his *personal* address, email address and telephone number. FAC ¶¶ 50-58. Plaintiff reasonably expected the foregoing to be kept private because he never consented to Twitter's interception, theft, scanning, collection, storage, and dissemination of it for Twitter's own financial and nefarious benefit. FAC ¶¶ 50-58. Moreover, to the extent the Court takes judicial notice of Defendant's exhibits, Exhibit C is purported to be a *private message* and contains his *business* phone number, and Exhibit D likewise references Plaintiff's *business* phone number and email. Plaintiff *never* made his private information including his *personal* phone number and email available.

Twitter's reliance on *In re Yahoo Mail Litigation*, 7. F. Supp. 3d 955 (N.D. Cal. 2015), to argue that Plaintiff fails to allege the requisite "specifics" misses the point. The constitutional right to privacy was adopted in part to protect the public from the stockpiling of personal information, and it is Twitter's wholesale scanning/theft of direct messages and confidential/privileged sources, and storage of users' private data, that Plaintiff alleges violates his reasonable expectation of privacy. Indeed, courts have warned of the privacy threat of prolonged surveillance, which collects

aggregated information about people.[15] Moreover, although *Yahoo* involved electronic messaging, the gravamen was that Yahoo used its subscribers' emails to extract information to target advertising. The *Yahoo* court focused on the fact that the plaintiff did not plead specific information that was "confidential" or "sensitive" because the "California Constitution protects only the *dissemination* or *misuses* of sensitive and confidential information." 7. F. Supp. 3d at 1040 (emphasis added) (citations omitted). Thus, because the plaintiff merely asserted that Yahoo was reading his emails to target advertising but failed to describe the specific content of the emails, there was no way to determine whether the content was sensitive/confidential and/or misused.

Compare *Yahoo* to *Mintz v. Mark Bartelstein & Assocs. Inc.,* 906 F. Supp. 2d 1017, 1034 (C.D. Cal. 2012) (finding viable constitutional privacy claim where the defendant breached former employee's computer simply because the defendant "deliberately accessed Plaintiff's Gmail account without permission, opened several emails, and even read their contents", irrespective of the specific contents); *see also Klayman v. Obama*, 957 F. Supp. 2d 1, 29-42 (D.D.C. 2013) (finding that although a person may not have a reasonable expectation of privacy in the phone numbers he/she dialed, they do however have "a very significant expectation of privacy in an aggregated collection of their telephone metadata" and the NSA's collection and searching of that metadata "significantly intrudes on that expectation."). Moreover, although in the context of

[15] *See*, *e.g.*, *U.S. v. Maynard,* 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd in prt sub nom U.S. v. Jones*, 132 S. Ct. 945 (2012) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups--and not just one such fact about a person, but all such facts.").

emails, California courts have recognized that the recipient of an email may "easily transmit the communication to anyone else who has access to the internet or print the communications," (*In re Google Inc. Gmail Litig.*, 2013 WL 5423918 *23 (N.D. Cal. 2013)), Congress, state legislatures, and the courts have always treated the unlawful interception of communications by a third-party differently.

Here, Plaintiff does not allege a privacy interest in his Twitter account in and of itself; rather, Plaintiff alleges a privacy interest in the private messages, confidential/privileged sources, list of followers and data Defendant unlawfully intercepted, reviewed, collected, stored, and disseminated for its own nefarious purposes. In fact, Twitter's conduct here is even more egregious than the defendants in both *Mintz* and *Klayman*, *supra*, because Twitter collected actual, confidential/privileged *content*, not simply metadata; *see also U.S. v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010) ("People are now able to send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away…In short, 'account' is an apt word for the conglomeration of stored messages that comprises an email account, as it provides an account of its owner's life."); *U.S. v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2007) (finding that the privacy interest in the content of email is the same as in the content of physical mail). Twitter's conduct was a far more serious invasion of privacy.

Finally, contrary to Defendant's argument, a Northern District of California court recently opined that the "offensiveness or seriousness of the intrusion, including any justification or other relevant interests" must be taken into account, and that "courts must be reluctant to reach a conclusion at the pleading stage about how offensive or serious the privacy intrusion is." *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1054 (N.D. Cal. 2018) (Whether conduct rises to the level of highly offensive is indeed a factual question best left for a jury) (internal quotations

omitted); *see also Opperman v. Path, Inc.*, 205 F. Supp. 3d 1064, 1080 (N.D. Cal. 2016) ("A judge should be cautious before substituting his or her judgment for that of the community."). Accordingly, the Court should deny Twitter's motion to dismiss Plaintiff's constitutional privacy claim.

**h. Plaintiff States a Claim For Unjust Enrichment**

Plaintiffs' cause of action for restitution based on quasi-contract/unjust enrichment is cognizable under California law as an alternative claim, and has repeatedly been recognized as such. *See Paracor Fin., Inc., v. GE Capital Corp.*, 96 F.3d 1151, 1167 (9th Cir. 1996) (holding that "unjust enrichment is an action in quasi-contract" under California law); *In re Hydroxycut Mktg. & Sales Practices Litig.*, 801 F.Supp.2d 993, 1010-12 (S.D.Cal. 2011) (holding that while California courts may "diverge on the proper way to conceptualize unjust enrichment," it is nevertheless a "claim" and a "basis for recovery"); *Astiana v. Ben & Jerry's Homemade, Inc.*, 2011 WL 2111796, at *11 (N.D.Cal. May 26, 2011) (denying the defendant's motion to dismiss in an "All Natural" case, holding that the plaintiffs could bring an unjust enrichment claim "as part of a claim of restitution based on quasi-contract" related to the plaintiffs' "all natural" false advertising claims); *see also Shum v. Intel Corp.*, 499 F.3d 1272, 1279 (Fed.Cir. 2007) (holding that unjust enrichment is a cognizable and "separate cause of action when the claim is grounded in equitable principles of restitution" under California law). This is in accord with long-standing California law. *See*, e.g., *Ghirardo v. Antonioli*, 924 P.2d 996, 1002-03 (Cal.1996) (acknowledging that, under California law, a party can seek relief "under traditional equitable principles of unjust enrichment"); *Boughton*, 20 Cal.Rptr.3d at 121-22 ("restitution may be awarded where the defendant obtained a benefit from the plaintiff by fraud, duress, conversion, or similar conduct. In such cases, the plaintiff may choose not to sue in tort, but instead to seek restitution on a quasi-contract theory"). Thus, Plaintiff has stated a viable claim for unjust enrichment.

**i. Plaintiff States a Claim For Negligence.**

"Causation in the law of negligence is not determined by a linear projection from a "but for" premise. Instead, it is expressed in terms of "foreseeability" and is limited by the policy that cause must be proximate. The problem is complex, and has bedeviled many. *Brewer v Teano*, 40 Cal App 4th 1024, 1030 (1995) (internal citations omitted). The question of foreseeability is often a question of fact for the jury. *Id*. Here, it was certainly foreseeable that Twitter's negligent failure to "implement policies, practices, and both procedural and oversight safeguards that could have, and would have, prevented the acts perpetrated by Alzabarah and Abouammo." Complaint at § 154. Twitter should not be rewarded for, at best, acting like an ostrich with its head in the sand.

**j. It is Well Established In California That The Effect Of Pleading And Proving A Conspiracy (As Applied Did In This Case) Is To Render All Those Who Cooperate In The Conspiracy Jointly Liable For All Damages With Those Who Actually Carry It Out.**

The law of conspiracy is equally well established in California. First, simple conspiracy is not an independent tort, but is a means of imposing joint liability on co-conspirators for conduct which is otherwise wrongful and tortious. "'It is the long established rule that conspiracy, in and of itself, however atrocious, does not give rise to a cause of action unless a civil wrong has been committed resulting in damage'... Hence, to state a cause of action for conspiracy, the complaint must allege (1) its formation and operation, (2) wrongful acts done pursuant thereto and (3) damages arising therefrom." *Olivet v. Frischling,* 104 Cal.App.3d 831, 837 (1980), quoting *Wise,* 223 Cal.App.2d at 64; *Rosenfeld, Meyer & Susman v. Cohen*, 146 Cal. App.3d 200 (1983).

Once a conspiracy to perform a tortious act is established, its "major significance ... lies in the fact that it renders each participant in the wrongful act responsible as a joint tortfeasor ... irrespective of whether or not he was a direct actor and regardless of the degree of his

activity." *Manor Investment Co. v. Wolworth*, 159 Cal.App.3d 586, 595 (1984). Proving a conspiracy "fasten[s] liability on him who agreed to the plan to commit the wrong as well as on him who carried it out." *Id.*; *see also Wyatt v. Union Mortgage Co.* (1979), 24 Cal.3d 773, 784-85.

**k. Plaintiff States A Claim For Replevin.**

Plaintiff "labeling his pleading as a petition for writ of replevin is "a relatively harmless historical observation." *Foster v. Sexton*, 61 Cal, App. 5th 998. As Defendant notes, in order to prove replevin/conversion, plaintiff must plead "(1) his ownership of or right to possess the property at the time of the conversion, (2) that the defendant disposed of the plaintiff's property rights or converted the property by a wrongful act, and (3) damages." *Bank of New York v. Fremont Gen. Corp.*, 523 F.3d 902, 914 (9th Cir. 2008). Defendant's allegation that Plaintiff cannot prove the first two elements is false.

1. First, while Defendant claims that there was nothing wrongful about its conduct, Plaintiff presents an entirely different narrative; namely, that Twitter assisted or, at the very least, authorized the unlawful hack and subsequent suspension of Plaintiff's account. Thus, whether or not Defendant engaged in "wrongful conduct" is a question of fact for the jury. Second, although Defendant claims that it owns Plaintiff's Twitter users and private data contained within his Twitter, this is nonsense. Plaintiff had the reasonable expectation that his proprietary sources, intellectual property, and user content used to build and generate his business, and stored on Twitter, were his property. Indeed, Defendant acknowledges that its TOS "*exclud[e] Content provided by users*." *See* Defendant's RJN, Ex. 6H § 7. This Content includes the proprietary sources, intellectual property, and user content used to build and generate his business. As Plaintiff's Complaint alleges, Twitter has "for far too long operated in the dark, accountable to no one, saying one thing while doing another without an iota of

transparency while donning a mantle of integrity and faux objectivity while converting amassed data to their own pecuniary purposes. Under principles of equity and good conscience Defendants should not be permitted to retain these lists or restrict or withhold access to this list of approximately 36,000 patrons of Plaintiff's journalistic and humanitarian coverage which Defendants have wrongfully withheld as a result of their unlawful actions and/or post-hoc rationalization sanctions." Complaint at ¶¶ 164-165.

## VI. REQUEST FOR LEAVE TO AMEND

If the Court grants all or part of Twitter's motion to dismiss, Plaintiff respectfully request leave to amend to address any such issues. All of Defendant's arguments, if found to have merit, would become moot if Plaintiff were to have leave to amend to address them.

## CONCLUSION

For the foregoing reasons, the Court should deny Plaintiff's motion in its entirety.

Dated: January 17, 2022

**GERSTMAN SCHWARTZ LLP**

By: /s/ *Randy E. Kleinman*
Randy E. Kleinman
1399 Franklin Avenue, Suite 200
Garden City, New York 11530
Telephone: (516) 880-8170
Facsimile: (516) 880-8171
rkleinman@gerstmanschwartz.com

*Attorneys for Plaintiff Ali Al-Ahmed*